MICHAEL KANS LAW

mdk@michaelkanslaw.com
www.michaelkans.com

This memorandum discusses, analyzes and summarizes the three write ups I did earlier this summer of the "Infrastructure Investment and Jobs Act" (H.R.3684) (aka the Bipartisan Infrastructure Bill or BIF). Since the House passed the Senate's bill without modification, all that I wrote over the summer has been enacted into law.

Bipartisan Infrastructure Package: Broadband

Last week, the Senate passed the "Infrastructure Investment and Jobs Act" (H.R.3684), sending the bill to the House. As has been widely reported, Congressional Democratic Leadership is linking this bill with a forthcoming $3.5 trillion package "to enact the [White House's] Build Back Better agenda." Consequently, this bill will likely not pass before the other package does unless it fails to pass. Then Democrats would be faced with a dilemma, for the $3.5 trillion package is probably the only opportunity to enact President Joe Biden's sweeping plans to address climate change, higher education, healthcare, and other Democratic policy priorities.

Putting aside the politics and probabilities, the Senate's $1 trillion infrastructure package is chock full of cybersecurity and technology funding and programmatic provisions. However, given the breadth of programs and funding, today we will just look at the very extensive broadband programs that carry a purported price tag of $65 billion, $35 billion less than the White House and Democratic stakeholders wanted.

Nonetheless, the drafters of much of the broadband language decided against using the Federal Communications Commission (FCC) as the conduit and overseer for most of the funds. Instead, the Department of Commerce's National Information and Telecommunications Administration (NTIA) will fill this role. There are likely a few reasons for this. First, Members have long wrangled with the agency just to get accurate maps of broadband coverage in the U.S. and over the definition of high-speed internet. There may not be a lot of patience or good feelings on Capitol Hill towards the FCC. Second, at present, the agency is deadlocked with 2 Democrats and 2 Republicans, and there have been no public signs as to when the Biden Administration will nominate a commissioner to tip the agency to the Democrats. Although a few theories have been floated as to why this is, including the White House not wanting to complicate passage of the infrastructure bill, infighting in the White House, giving acting Chair Jessica Rosenworcel a "try out," and cross currents from Democratic stakeholders about a nominee. Third, the NTIA will be more answerable to the White House through the Secretary of Commerce and department senior officials. Moreover, Secretary Gina Raimondo has earned raves form key moderate Senators, and as a former governor she is presumably experienced in the view from a statehouse in trying to fulfill dictates from Washington.

The Senate folded provisions from the "Accessible, Affordable Internet for All Act" (H.R.1783/S.745) (see here for more detail on the bill as introduced) but reduced the overall funding from $94 billion to $65 billion, largely in the form of a new grant program the National Telecommunications and Information Administration (NTIA) would

administer. The agency must establish within six months a "Broadband Equity, Access, and Deployment Program" to make grants to eligible entities, and $42.45 billion is authorized and appropriated for this program. The NTIA "shall provide technical support and assistance to eligible entities (a term defined to include only states, the District of Columbia and certain U.S. territories) to facilitate their participation in the Program, including by assisting eligible entities with—

> *(i) the development of grant applications under the Program;*
> *(ii) the development of plans and procedures for distribution of funds under the Program; and*
> *(iii) other technical support as determined by the [NTIA].*

The NTIA is also charged with providing more general assistance to states for obtaining a Broadband Equity, Access, and Deployment Program grant, namely:

> *(i) to support the expansion of broadband, with priority for—*
> > *(I) expansion in rural areas; and*
> > *(II) eligible entities that consistently rank below most other eligible entities with respect to broadband access and deployment; and*
> *(ii) regarding cybersecurity resources and programs available through Federal agencies, including the Election Assistance Commission, the Cybersecurity and Infrastructure Security Agency, the Federal Trade Commission, and the National Institute of Standards and Technology.*

The NTIA would make grants based on a formula determined by the FCC's broadband maps as required by the "Broadband DATA Act" (P.L. 116-130) (47 U.S.C. 642 et seq.). On 6 August, the FCC announced "a brand-new map showing mobile coverage and availability data in the U.S. from the country's largest wireless providers." The agency continued that "[t]his is the first public map showing updated mobile coverage released by the FCC and represents a significant improvement over other data previously published by the agency." The FCC added the map "also serves as a public test of the standardized criteria developed to facilitate improved mapping under the Broadband DATA Act." It is not clear whether this broadband map that features only data voluntarily submitted by the four biggest wireless carriers in the U.S. suffices to satisfy the Broadband DATA Act's requirements. It bears note that the bill refers to broadband data maps and not a map, suggesting the FCC has some other maps to draft and publish. Consequently, NTIA may need to wait on the FCC's completion of the broadband map mandated under the Broadband DATA Act to disburse the $42.45 billion in grant funding aimed at rural and underserved areas of the U.S. to close to digital divide. Or expediency and political pressure may encourage the NTIA to deem the 6 August map sufficient and proceed.

In any event, once the Broadband DATA Act maps are finished and published, the NTIA must allocate $4.245 billion to states with none receiving less than $100 million with the United States Virgin Islands, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands dividing a total of $100 million. The NTIA needs to use a formula to distribute funds for this first tranche, and this formula requires:

- "dividing the number of unserved locations in high-cost areas in the eligible entity by the total number of unserved locations in high-cost areas in the United States" and
- Multiplying this number by $4.245 billion

The rest of these funds ($38.205 billion) will be distributed thorough a different formula:

- "(i) dividing the number of unserved locations in the eligible entity by the total number of unserved locations in the United States; and"
- Multiplying this number by $38.205 billion

Moreover, within six months of enactment the NTIA must issue a notice of funding opportunity for the Broadband Equity, Access, and Deployment Program and after states submit letters of intent, they can apply for planning grants, which could be no more than 5% of the second tranche of funds. In exchange for these planning funds, states will need to complete three-year action plans.

When the NTIA can start handing out funds, states will need to navigate and complete a lengthy application process designed, no doubt, to ensure NTIA can ensure funds will be well used for the purposes of the act.

Be that as it may, when funding is doled out, states would then make competitive grants to subgrantees for

- *unserved service projects and underserved service projects;*
- *connecting eligible community anchor institutions;*
- *data collection, broadband mapping, and planning;*
- *installing internet and Wi-Fi infrastructure or providing reduced-cost broadband within a multi-family residential building, with priority given to a residential building that—*
    - *has a substantial share of unserved households; or*
    - *is in a location in which the percentage of individuals with a household income that is at or below 150 percent of the poverty line applicable to a family of the size involved (as determined under section 673(2) of the Community Services Block Grant Act (42 U.S.C. 9902(2)) is higher than the national percentage of such individuals;*
- *broadband adoption, including programs to provide affordable internet-capable devices; and*
- *any use determined necessary by [NTIA] to facilitate the goals of the Program.*

And so, obviously, these funds would be directed first and foremost to entities looking to bridge broadband gaps or limited service. There are other purposes for which entities could use funds, including for Wi-Fi infrastructure in multi-family residential buildings or for reduced price service.

Moreover, all subgrantees

- *shall adhere to quality-of-service standards, as established by [NTIA];*

- *shall comply with prudent cybersecurity and supply chain risk management practices, as specified by [NTIA], in consultation with the Director of the National Institute of Standards and Technology and the Commission;*
- *shall incorporate best practices, as defined by [NTIA], for ensuring reliability and resilience of broadband infrastructure; and*
- *may not use the amounts to purchase or support—*
    - *any covered communications equipment or service, as defined in section 9 of the Secure and Trusted Communications Networks Act of 2019 (47 U.S.C. 1608); or*
    - *fiber optic cable and optical transmission equipment manufactured in the People's Republic of China, except that [NTIA] may waive the application of this clause with respect to a project if the eligible entity that awards a subgrant for the project shows that such application would unreasonably increase the cost of the project.*

The Senate is looking to further bake restrictions into U.S. telecommunications law and systems through the latter of these provisions. The FCC's program to protect the U.S. telecommunications system against national security threats (mainly equipment and services from the PRC) bars the use of Universal Service Fund (USF) dollars from buying banned equipment and services. The above language would essentially extend this ban to the $42.45 billion in broadband grant funds. But it also expands the ban to include fiber optic cable and optical transmission equipment made in the PRC with the caveat that NTIA may waive this provision on the basis of increased costs, meaning there are not cheaper or equivalent options available.

The bill would also piggyback better broadband cybersecurity and supply chain risk management by conditioning the funds on meeting standards to be promulgated by NTIA, NIST, and the FCC. The same would be true of broadband infrastructure reliability and resilience.

States would need to award funds for broadband networks based on these criteria:

> *(i) shall award funding in a manner that—*
> *(I) prioritizes unserved service projects;*
> *(II) after certifying to [NTIA] that the eligible entity will ensure coverage of broadband service to all unserved locations within the eligible entity, prioritizes underserved service projects; and*
> *(III) after prioritizing underserved service projects, provides funding to connect eligible community anchor institutions;*
> *(ii) in providing funding under subclauses (I), (II), and (III) of clause (i), shall prioritize funding for deployment of broadband infrastructure for priority broadband projects;*
> *(iii) may not exclude cooperatives, nonprofit organizations, public-private partnerships, private companies, public or private utilities, public utility districts, or local governments from eligibility for such grant funds; and*
> *(iv) shall give priority to projects based on—*
> *(I) deployment of a broadband network to persistent poverty counties or high-poverty areas;*
> *(II) the speeds of the proposed broadband service;*

(III) the expediency with which a project can be completed; and
(IV) a demonstrated record of and plans to be in compliance with Federal labor and employment laws.

So, the funds would be provided to projects that help unserved areas, then underserved areas, and finally to "eligible community anchor institutions" (a term that includes a number of institutions like schools, libraries, public housing organization, and others that lack gigabit-level broadband service.) But further preference would be given to "priority broadband projects" which are "designed to—

(i) provide broadband service that meets speed, latency, reliability, consistency in quality of service, and related criteria as the [NTIA] shall determine; and (ii) ensure that the network built by the project can easily scale speeds over time to—
(I) meet the evolving connectivity needs of households and businesses; and
(II) support the deployment of 5G, successor wireless technologies, and other advanced services.

As a result, the NTIA will almost certainly need to publish guidance or even more likely conduct a rulemaking to define the specifications that projects must meet in order to be "priority broadband projects."

The eligible group of subgrantees would seem to include every possible stakeholder interested in receiving broadband funds. Nonetheless, additional priority would be given to those projects that would bring broadband to poor areas, the speed of the proposed service, how quickly the project can be reasonably completed, and the entity's record of complying with federal labor and employment laws.

In sum, it appears the highest preference would go to projects to provide broadband to unserved areas with high levels of poverty for priority broadband projects.

For the deployment of broadband networks, subgrantees would need to match federal funds with 25% of the project costs except for high-cost areas and in some other cases. The non-federal match can come from a variety of sources, including recently funds leftover from COVID-19 appropriations packages.

The NTIA would also establish means to claw back funds from non-performing subgrantees in consultation with federal and state partners.

The NTIA and FCC would have two years to stand up a publicly website that:

(i) allows a consumer to determine, based on financial information entered by the consumer, whether the consumer is eligible—
(I) to receive a Federal or State subsidy with respect to broadband service; or
(II) for a low-income plan with respect to broadband service; and
(ii) contains information regarding how to apply for the applicable benefit described in clause (i).

Additionally, "[a] Federal entity, State entity receiving Federal funds, or provider of broadband service that offers a subsidy or low-income plan, as applicable, with respect

to broadband service shall provide data to the [NTIA} in a manner and format as established by the [NTIA] as necessary."
The Senate has also set a very high bar for any legal challenges of any NTIA decisions. First, the federal court in Washington DC is the only court that can hear such cases, and it must rule for the NTIA unless:

- *the decision was procured by corruption, fraud, or undue means;*
- *there was actual partiality or corruption in the Assistant Secretary; or*
- *the Assistant Secretary was guilty of—*
    - *misconduct in refusing to review the administrative record; or*
    - *any other misbehavior by which the rights of any party have been prejudiced.*

In short, unless NTIA engaged in illegal behavior or a flagrant disregard of administrative claims, its decisions in the $42.45 billion broadband program cannot be challenged.

The FCC's remit and authority under the "Broadband DATA Act" would be changed. Broadband providers would be required to provide the information and data the agency needs to create broadband maps. The FCC would also be required to commence a proceeding on how the agency is to achieve universal service for broadband goals in light of passage of the act. The FCC would need to report to Congress on how its efficiency in achieving universal service could be improved. The FCC is moreover tasked with establishing an online mapping tool within 18 months "to provide a locations overview of the overall geographic footprint of each broadband infrastructure deployment project funded by the Federal Government."

The bill removes limits on the "Tribal Broadband Connectivity Program" established in the "Consolidated Appropriations Act, 2021" (P.L.116–260), and $2 billion more is appropriated for this program. The NTIA is in the process of disbursing the $980 million made available for FY 2021.

The "Infrastructure Investment and Jobs Act" includes another broadband bill, the "Digital Equity Act of 2021" (H.R.1841/S.2018) would establish the State Digital Equity Capacity Grant and the Digital Equity Competitive Grant Programs and provide $2.75 billion in total for them.

The NTIA would establish the State Digital Equity Capacity Grant Program

- *the purpose of which is to promote the achievement of digital equity, support digital inclusion activities, and build capacity for efforts by States relating to the adoption of broadband by residents of those States;*
- *through which the Assistant Secretary shall make grants to States in accordance with the requirements of this section; and*
- *which shall ensure that States have the capacity to promote the achievement of digital equity and support digital inclusion activities.*

States would select an entity to administer the program, and those eligible for this task include a range of entities such as the state government itself, a political subdivision, a Tribal government, foundation, corporation, an educational agency and others.

Each state that wants to participate would need to draft a State Digital Equity Plan that, among other components, identifies obstacles to full digital equity, goals to promote inclusion among a number of groups, and the interplay of digital equity and other state planning processes for health, labor, education, and others. The NTIA shall award planning grants to states to execute their equity plans. Two years after the process of making planning grants starts, NTIA would start awarding state capacity grants to implement states' digital equity plans and other measures to increase digital inclusion. A total of $600 million is provided for the two grant programs with $60 million being for planning grants. The bill outlines a formula for the distribution of the funds: 50% will be provided based on a state's population in proportion to the U.S. population; 25% will be given based on the number of people in covered populations (i.e. those groups among whom there is less digital engagement such as the elderly and people who are learning English); and 25% based on the comparative lack of broadband availability and adoption in proportion to the broadband availability and adoption in all eligible states. NTIA may terminate and redistribute grant funds if states fail to use the proceeds in the ways they have agreed to.

The NTIA would also establish the Digital Equity Competitive Grant Program "the purpose of which is to award grants to support efforts to achieve digital equity, promote digital inclusion activities, and spur greater adoption of broadband among covered populations." Those entities eligible for this grant are similar to those that can receive state capacity grants under the State Digital Equity Plan. When considering applications for this grant program, the NTIA "shall, to the extent practicable, consider—

- *whether an application shall, if approved—*
    - *increase internet access and the adoption of broadband among covered populations to be served by the applicant; and*
    - *not result in unjust enrichment;*
- *the comparative geographic diversity of the application in relation to other eligible applications; and*
- *the extent to which an application may duplicate or conflict with another program.*"

The grants will support at least one of the following:

- *To develop and implement digital inclusion activities that benefit covered populations.*
- *To facilitate the adoption of broadband by covered populations in order to provide educational and employment opportunities to those populations.*
- *To implement, consistent with the purposes of this title—*
    - *training programs for covered populations that cover basic, advanced, and applied skills; or*
    - *other workforce development programs.*
- *To make available equipment, instrumentation, networking capability, hardware and software, or digital network technology for broadband services to covered populations at low or no cost.*
- *To construct, upgrade, expend, or operate new or existing public access computing centers for covered populations through community anchor institutions.*
- *To undertake any other project and activity that the Assistant Secretary finds to be consistent with the purposes for which the Program is established.*

This grant program will require at least a 10% non-federal match and perhaps even more, for the language in the bill caps the federal portion at 90% and suggests NTIA could reduce the federal share even further at its discretion. NTIA may grants waivers for the non-federal share, however.

$1.25 billion is provided for the Digital Equity Competitive Grant Program, 5% of which may be kept by NTIA to finance administration, 5% of which shall go to grants or agreements with Indian Tribes, Alaska Native entities, and Native Hawaiian organizations, and 1% of which shall go to the United States Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any other territory or possession of the United States that is not a State.

The "Infrastructure Investment and Jobs Act" establishes another broadband development program. The NTIA "shall establish a program under which the [NTIA] makes grants on a technology-neutral, competitive basis to eligible entities for the construction, improvement, or acquisition of middle mile infrastructure." $1 billion is provided for this new program, and the purpose of this program is:

- *to encourage the expansion and extension of middle mile infrastructure to reduce the cost of connecting unserved and underserved areas to the backbone of the internet (commonly referred to as the ''last mile''); and*
- *to promote broadband connection resiliency through the creation of alternative network connection paths that can be designed to prevent single points of failure on a broadband network.*

The NTIA will be able to make grants to further build middle mile infrastructure to the following entities:

> *a State, political subdivision of a State, Tribal government, technology company, electric utility, utility cooperative, public utility district, telecommunications company, telecommunications cooperative, nonprofit foundation, non-profit corporation, nonprofit institution, non-profit association, regional planning counsel, Native entity, or economic development authority*

NTIA is to prioritize applications from eligible entities that do two or more of the following:

- *The eligible entity adopts fiscally sustainable middle mile strategies.*
- *The eligible entity commits to offering non-discriminatory interconnect to terrestrial and wireless last mile broadband providers and any other party making a bona fide request.*
- *The eligible entity identifies specific terrestrial and wireless last mile broadband providers that have—*
    - *expressed written interest in interconnecting with middle mile infrastructure planned to be deployed by the eligible entity; and*
    - *demonstrated sustainable business plans or adequate funding sources with respect to the interconnect described in clause (i).*

- *The eligible entity has identified supplemental investments or in-kind support (such as waived franchise or permitting fees) that will accelerate the completion of the planned project.*
- *The eligible entity has demonstrated that the middle mile infrastructure will benefit national security interests of the United States and the Department of Defense.*

Moreover,

> *A project shall be eligible for a middle mile grant if, at the time of the application, the [NTIA] determines that the proposed middle mile broadband network will be capable of supporting retail broadband service.*

Finally, under the Middle Mile Infrastructure Grant Program, the U.S. government cannot pay for more than 70% of a project, and so the applicant must finance at least 30%.

Another COVID-19 relief program from the "Consolidated Appropriations Act, 2021" (P.L.116–260) is refashioned and extended. The "Benefit For Broadband Service During Emergency Period Relating To COVID-19" would become the "Affordability Connectivity" program. $14.2 billion will be given to the FCC for this program that reimburses internet service providers mainly for providing low cost service to certain households. There are provisions that would revise some aspects of the program, including language for ISPs to recover more costs for providing service in high-cost areas on Tribal lands. Moreover, providers must allow eligible people to choose any of the ISP's regularly offered plans and cannot require a credit check. Moreover, when a customer subscribes or renews a subscription, the ISP must tell them about the Affordability Connectivity program and how to enroll. Additionally, the FCC will need to promulgate rules to protect consumers from a number of ISP practices, including inappropriate upselling or downselling, inappropriate requirements that customers using this benefit sign on for extended contracts, inappropriate restrictions on switching ISPs while using the benefit, and "similar restrictions that amount to unjust and unreasonable acts or practices that undermine the purpose, intent, or integrity of the Affordable Connectivity Program."

The FCC will need to certify it has disbursed all benefit funds distributed under the predecessor program before it can start handing out the new funds. Additionally, eligibility will be increased by making households earning up to 200% of the Federal Poverty Guidelines and through revising upward other criteria. However, the per-month dollar amount for households would decrease from $50 to $30.

One year after enactment of the "Infrastructure Investment and Jobs Act," the FCC must promulgate "regulations to require the display of broadband consumer labels, as described in the Public Notice of the Commission issued on April 4, 2016 (DA 16–357), to disclose to consumers information regarding broadband internet access service plans. During the Trump Administration FCC, in repealing the Obama Administration's FCC's net neutrality rules, it also rolled back broadband labeling rules. Recently, Consumer Reports' Digital Lab announced an effort to bootstrap broadband labeling. The organization stated that "along with a coalition of partners, is embarking on an ambitious project called Broadband Together to investigate the state of internet access in the U.S…[and] will analyze thousands of consumer ISP bills from across the country to better understand

what factors determine why and how ISPs charge the prices they do, and what information is and is not included in monthly bills."

Within two years, the FCC must also "adopt final rules to facilitate equal access to broadband internet access service, taking into account the issues of technical and economic feasibility presented by that objective, including—

- *preventing digital discrimination of access based on income level, race, ethnicity, color, religion, or national origin; and*
- *identifying necessary steps for the Commissions to take to eliminate discrimination described in paragraph (1).*"

The bill also includes the "Telecommunications Skilled Workforce Act" (H.R.1032/S.163) that establishes a "Telecommunications Interagency Working Group" "to address the workforce needs of the telecommunications industry, including the safety of that workforce." This Task Force would develop and make recommendations to Congress. In a related directive, the Department of Labor and the FCC must:

> *issue guidance on how States can address the workforce needs and safety of the telecommunications industry, including guidance on how a State workforce development board established under section 101 of the Workforce Innovation and Opportunity Act (29 U.S.C. 3111) can—*
>
> > *(1) utilize Federal resources available to States to meet the workforce needs of the telecommunications industry;*
> >
> > *(2) promote and improve recruitment in workforce development programs in the telecommunications industry; and*
> >
> > *(3) ensure the safety of the telecommunications workforce, including tower climbers.*

The "Infrastructure Investment and Jobs Act" expands qualified private activity bonds (PAB) to include broadband projects as a means of fostering private sector investment. These provisions are based on the "Rural Broadband Financing Flexibility Act" (S.1676), and the Joint Committee on Taxation has estimated this would cost $566 million in lost revenue, and at least one summary is claiming it will provide $600 million in broadband projects. For those not versed in PABs (like me), here is a handy summary the Internal Revenue Service issued:

> *Interest on State and local government bonds is taxable if the bonds are private activity bonds (bonds issued to finance private activities not specifically authorized by Congress) unless the bond is a qualified private activity bond provided for in the Code.*

The bill defines "qualified broadband projects" as "any project which—

- *is designed to provide broadband service solely to 1 or more census block groups in which more than 50 percent of residential households do not have access to fixed, terrestrial broadband service which delivers at least 25 megabits per second downstream and at least 3 megabits service upstream, and*

- *results in internet access to residential locations, commercial locations, or a combination of residential and commercial locations at speeds not less than 100 megabits per second for downloads and 20 megabits for second for uploads, but only if at least 90 percent of the locations provided such access under the project are locations where, before the project, a broadband service provider—*
    - *did not provide service, or*
    - *did not provide service meeting the minimum speed requirements described in subparagraph (A).*

There are other requirements in using a PAB to finance a qualified broadband project, too.

The Department of Agriculture's Rural Utilities Service's Distance Learning, Telemedicine, and Broadband Program would be given $2 billion in additional funding for broadband loans and grants subject to extensive conditions spelled out in the bill, including coordination with the NTIA and FCC.

Bipartisan Infrastructure Package: Drinking Water and The Grid

Recently, the Senate passed the "Infrastructure Investment and Jobs Act" (H.R.3684), sending the bill to the House. This bill is teeming with technology funding and policy, the likes of which could alter United States (U.S.) policy in a number of realms for years to come. We looked at the broadband provisions in the last issue (see here), and today, we will examine the provisions and funding related to drinking water systems, the electric grid, and related technology.

The Senate included language and funding to address the vulnerabilities turned up by this year's high-profile attack of a Florida drinking water facility. This sort of attack and the vulnerabilities many water facilities around the globe have is not new, for there was an attack in 2000 in Australia. Nonetheless, this year's attack caught the attention of U.S. policymakers. The following provisions were largely pulled from the Senate Environment and Public Works Committee's "Drinking Water and Wastewater Infrastructure Act of 2021" (S.914).

In Division E "Drinking Water and Wastewater Infrastructure," the U.S. Environmental Protection Agency (EPA) is tasked with establishing the "Midsize and Large Drinking Water System Infrastructure Resilience and Sustainability Program" under which the agency "shall award grants to eligible entities for the purpose of—

- *increasing resilience to natural hazards and extreme weather events; and*
- *reducing cybersecurity vulnerabilities.*

Those public water facilities eligible for such grants are those that serve a population of 10,000 or more. It bears emphasis this program appears to merely be authorized at $50 million a year over the next five fiscal years with no funds actually appropriated. This would be presumably up to the Appropriations Committees to address in annual bills.

The EPA would also need to "carry out a study that examines the state of existing and potential future technology, including technology that could address cybersecurity

vulnerabilities, that enhances or could enhance the treatment, monitoring, affordability, efficiency, and safety of drinking water provided by a public water system." After reporting to Congress, the EPA must establish a competitive grant program "for the purpose of identifying, deploying, or identifying and deploying technologies" that are advanced, including those pertaining to cybersecurity.

Public water systems that serve 100,000 and fewer people are eligible to apply, and the federal share is capped at 90% of costs. $10 million is authorized for each of the next five fiscal years but again not appropriated.

A new section is added to the "Safe Drinking Water Act" (42 U.S.C. 300g et seq.): "Cybersecurity Support For Public Water Systems." The EPA must coordinate with the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) in developing "a prioritization framework to identify public water systems (including sources of water for those public water systems) that, if degraded or rendered inoperable due to an incident, would lead to significant impacts on the health and safety of the public." Within nine months of enactment, the "[EPA], in coordination with [CISA] and using existing authorities of the [EPA] and [CISA] for providing voluntary support to public water systems and the Prioritization Framework, shall develop a Technical Cybersecurity Support Plan for public water systems." And yet, the section goes out the way to stress that nothing in this new program shall compel a public water system to comply with any EPA technical support. So, again, a voluntary program that offers increased resources and focus on cybersecurity that critical infrastructure owners and operators are free to disregard.

The EPA would moreover need to establish a new "Clean Water Infrastructure Resiliency and Sustainability Program" in order to "award grants to eligible entities for the purpose of increasing the resilience of publicly owned treatment works to a natural hazard or cybersecurity vulnerabilities." Municipalities and state agencies can apply for funds and "shall use the grant funds for planning, designing, or constructing projects (on a system-wide or area-wide basis) that increase the resilience of a publicly owned treatment works to a natural hazard or cybersecurity vulnerabilities." The EPA cannot pay for more than 75% of the project except for public water systems that serve 10,000 or fewer people and other criteria at which point the federal share can be as high as 90%. $25 million a year for five fiscal years is authorized but not appropriated for this new program.

The EPA must "develop best practices that may be implemented by State, Tribal, and local governments with respect to the collection of batteries to be recycled in a manner that—

- *to the maximum extent practicable, is technically and economically feasible for State, Tribal, and local governments;*
- *is environmentally sound and safe for waste management workers; and*
- *optimizes the value and use of material derived from recycling of batteries.*"

$10 million would be made available for this program.

The EPA would need to stand up a program "to promote battery recycling through the development of—

- *voluntary labeling guidelines for batteries; and*
- *other forms of communication materials for battery producers and consumers about the reuse and recycling of critical materials from batteries."*

And the EPA would receive $15 million for the voluntary labeling guidelines program.

There are numerous Department of Energy (DOE) technology provisions, most of which relate to the cybersecurity of the U.S. electric grid.

DOE would need to establish a new program for states to draft and implement State Energy Security Plans. Additionally, DOE can provide financial assistance for states "for the development, implementation, review, and revision of a State energy security plan that—

- *assesses the existing circumstances in the State; and*
- *proposes methods to strengthen the ability of the State, in consultation with owners and operators of energy infrastructure in the State—*
    - *to secure the energy infrastructure of the State against all physical and cybersecurity threats;*
    - *to mitigate the risk of energy supply disruptions to the State; and*
    - *to enhance the response to, and recovery from, energy disruptions; and*
    - *to ensure that the State has reliable, secure, and resilient energy infrastructure.*

Governors must submit annual reports that meet the department's requirements, any necessary revisions to her state energy security plan and certification as to the need for these revisions. DOE and DHS are permitted to provide technical assistance to states.

The second section of the energy part of the bill deals with cybersecurity and supply chain risk management.

The DOE must establish a program to enhance grid security through public-private partnerships in coordination with DHS and "the heads of other relevant Federal agencies, State regulatory authorities, industry stakeholders, and the Electric Reliability Organization" (i.e. the North American Electric Reliability Corporation) as DOE sees fit. DOE and its partners must carry out a program:

- *to develop, and provide for voluntary implementation of, maturity models, self-assessments, and auditing methods for assessing the physical security and cybersecurity of electric utilities;*
- *to assist with threat assessment and cybersecurity training for electric utilities;*
- *to provide technical assistance for electric utilities subject to the program;*
- *to provide training to electric utilities to address and mitigate cybersecurity supply chain management risks;*
- *to advance, in partnership with electric utilities, the cybersecurity of third-party vendors that manufacture components of the electric grid;*

- *to increase opportunities for sharing best practices and data collection within the electric sector; and*
- *to assist, in the case of electric utilities that own defense critical electric infrastructure (as defined in section 215A(a) of the Federal Power Act (16 U.S.C. 824o–1(a))), with full engineering reviews of critical functions and operations at both the utility and defense infrastructure levels—*
    - *to identify unprotected avenues for cyber-enabled sabotage that would have catastrophic effects to national security; and*
    - *to recommend and implement engineering protections to ensure continued operations of identified critical functions even in the face of constant cyber attacks and achieved perimeter access by sophisticated adversaries.*

DOE must report to Congress one year after enactment on the cybersecurity of electricity distribution systems. DOE is also charged with safeguarding any information it collects or is provided that could endanger the U.S. electric grid. Consequently, this information cannot be disclosed not even for Freedom of Information Act (FOIA) requests.

The DOE will establish a voluntary Energy Cyber Sense program in conjunction with DHS and the other federal agencies. This new program will be developed "to test the cybersecurity of products and technologies intended for use in the energy sector, including in the bulk-power system" and including "industrial control systems and operational technologies, such as supervisory control and data acquisition systems." DOE must maintain a database of these products and the test results that "are integrated with Federal vulnerability coordination processes." The agency will provide technical assistance to remedy vulnerabilities in tested products and technology. DOE must develop guidance based on its testing for the electric sector on buying products and technology and consider incentives to drive the use of the testing results in how products and technology are designed and built. Finally, if the DOE reasonably foresees the disclosure of information related to this program could jeopardizes the physical or cybersecurity of the energy sector, she can exempt such information from FOIA and other public disclosure laws.

The Federal Energy Regulatory Commission (FERC) must "conduct a study to identify incentive-based, including performance-based, rate treatments for the transmission and sale of electric energy subject to the jurisdiction of the Commission that could be used to encourage—

- *investment by public utilities in advanced cybersecurity technology; and*
- *participation by public utilities in cybersecurity threat information sharing programs.*"

One year after this study is finished, FERC must "establish, by rule, incentive-based, including performance-based, rate treatments for the transmission of electric energy in interstate commerce and the sale of electric energy at wholesale in interstate commerce by public utilities for the purpose of benefitting consumers by encouraging" investment in advanced cybersecurity technology and the participation of public utilities in "cybersecurity threat information sharing programs." FERC may also provide other incentives to reduce risks to defense critical electric infrastructure and "facilities of small or medium-sized public utilities with limited cybersecurity resources."

The DOE must establish the "Rural and Municipal Utility Advanced Cybersecurity Grant and Technical Assistance Program" "to provide grants and technical assistance to, and enter into cooperative agreements with, eligible entities to protect against, detect, respond to, and recover from cybersecurity threats." This new program's objectives are:

- *to deploy advanced cybersecurity technologies for electric utility systems; and*
- *to increase the participation of eligible entities in cybersecurity threat information sharing programs.*

The entities eligible for this program are

(A) a rural electric cooperative;
(B) a utility owned by a political subdivision of a State, such as a municipally owned electric utility;
(C) a utility owned by any agency, authority, corporation, or instrumentality of 1 or more political subdivisions of a State;
(D) a not-for-profit entity that is in a partnership with not fewer than 6 entities described in subparagraph (A), (B), or (C); and
(E) an investor-owned electric utility that sells less than 4,000,000 megawatt hours of electricity per year.

DOE should prioritize grants and technical assistance to those entities with limited cybersecurity resources or own assets critical to the bulk power system or own defense critical electric infrastructure.

$250 million would be appropriated in $50 million chunks for each of the next five years.

DOE must carry out a program to enhance grid security to achieve the following (i.e., the "Cybersecurity for the Energy Sector Research, Development, and Demonstration Program"):

- *to develop advanced cybersecurity applications and technologies for the energy sector—*
    - *to identify and mitigate vulnerabilities, including—*
        - *dependencies on other critical infrastructure;*
        - *impacts from weather and fuel supply;*
        - *increased dependence on inverter-based technologies; and*
        - *vulnerabilities from unpatched hardware and software systems; and*
    - *to advance the security of field devices and third-party control systems, including—*
        - *systems for generation, transmission, distribution, end use, and market functions;*
        - *specific electric grid elements including advanced metering, demand response, distribution, generation, and electricity storage;*
        - *forensic analysis of infected systems;*
        - *secure communications; and*
        - *application of in-line edge security solutions;*

- *to leverage electric grid architecture as a means to assess risks to the energy sector, including by implementing an all-hazards approach to communications infrastructure, control systems architecture, and power systems architecture;*
- *to perform pilot demonstration projects with the energy sector to gain experience with new technologies;*
- *to develop workforce development curricula for energy sector-related cybersecurity; and*
- *to develop improved supply chain concepts for secure design of emerging digital components and power electronics.*

$50 million a year is appropriated annually for five fiscal years.

The DOE would be given the discretion to develop and execute a cyber-resilience program to test agency response capabilities and coordination with the National Laboratories and other agencies. DOE could also investigate enhanced threat sharing with the Intelligence Community and other purposes designed to foster greater cyber-resilience. $50 million would be appropriated annually for the next five fiscal years.

DOE would need to put in place "an advanced energy security program to secure energy networks, including…electric networks…natural gas networks; and…oil exploration, transmission, and delivery networks." The goal of this program is "to increase the functional preservation of electric grid operations or natural gas and oil operations in the face of natural and human-made threats and hazards, including electric magnetic pulse and geo-magnetic disturbances." This program would also be authorized for annual appropriations of $50 million for the next five fiscal years.

DOE may, in its discretion, require any recipient of funds for the aforementioned programs to

- *…submit…a cybersecurity plan that demonstrates the cybersecurity maturity of the recipient in the context of the project for which that award or other funding was provided; and*
- *establish a plan for maintaining and improving cybersecurity throughout the life of the proposed solution of the project.*

The Senate then addresses supply chain issues, a policy area that has come to the fore in Washington following a number of recently successful supply chain attacks. The United States Geological Survey (USGS) would need to establish an Earth Mapping Resources Initiative "to accelerate efforts to carry out the fundamental resources and mapping mission of the" USGS. The DOE must "through an agreement with an academic partner, the design, construction, and build-out of a facility to demonstrate the commercial feasibility of a full-scale integrated rare earth element extraction and separation facility and refinery." There are provisions directing the Department of the Interior to speed up the review of permitting for critical mineral production on federal lands.

The Senate sponsors are also interested in shoring up and fostering U.S. production of advanced batteries, a field in which the PRC is far ahead of the U.S. The Biden Administration conducted a review of U.S. supply chains, including a focus on advanced batteries, and then launched a number of initiatives based on its findings such as

"immediate actions [the DOE] will take to make the U.S. more competitive in the battery market."

On the heels of the White House's actions, the DOE would be required to "establish within the Office of Fossil Energy a program, to be known as the "Battery Material Processing Grant Program" to make grants

- *to ensure that the United States has a viable battery materials processing industry to supply the North American battery supply chain;*
- *to expand the capabilities of the United States in advanced battery manufacturing;*
- *to enhance national security by reducing the reliance of the United States on foreign competitors for critical materials and technologies; and*
- *to enhance the domestic processing capacity of minerals necessary for battery materials and advanced batteries.*

The DOE would make grants to the following entities:

- *to carry out 1 or more demonstration projects in the United States for the processing of battery materials;* (at least $50 million per grant)
- *to construct 1 or more new commercial-scale battery material processing facilities in the United States;* (at least $100 million per grant) *and*
- *to retool, retrofit, or expand 1 or more existing battery material processing facilities located in the United States and determined qualified by the Secretary* (at least $50 million per grant.)

$3 billion is appropriated for the "Battery Material Processing Grant Program" in $600 million amounts for each of the next five fiscal years.

In addition, the DOE will be tasked with establishing "within the Office of Energy Efficiency and Renewable Energy a "Battery Manufacturing and Recycling Grant Program," the purpose of which "is to ensure that the United States has a viable domestic manufacturing and recycling capability to support and sustain a North American battery supply chain. Grants would be given to eligible entities:

- *to carry out 1 or more demonstration projects for advanced battery component manufacturing, advanced battery manufacturing, and recycling;* (at least $50 million per grant)
- *to construct 1 or more new commercial-scale advanced battery component manufacturing, advanced battery manufacturing, or recycling facilities in the United States;* (at least $100 million per grant)and
- *to retool, retrofit, or expand 1 or more existing facilities located in the United States and determined qualified by the Secretary for advanced battery component manufacturing, advanced battery manufacturing, and recycling* (at least $50 million per grant.)

$3 billion is appropriated for the "Battery Material Processing Grant Program" in $600 million amounts for each of the next five fiscal years.

For both programs, DOE is to give priority in making grants to eligible entities located and operating in the U.S., owned by a U.S. entity, using U.S. or North American intellectual property and content, whether it will foster job creation in low and moderate income communities, helps replace jobs lost from the fossil fuels fields, partnership with Tribal entities, and the effect on greenhouse gas emissions, among others.

The "Infrastructure Investment and Jobs Act" directs the DOE to "continue to carry out the Lithium-Ion Battery Recycling Prize Competition, an already existing program, and authorizes and appropriates $10 million to conduct Phase III.

The DOE would be tasked with establishing another battery program. The agency would need to "award multiyear grants to eligible entities for research, development, and demonstration projects to create innovative and practical approaches to increase the reuse and recycling of batteries, including by addressing" some of the following, among other considerations:

- *recycling activities;*
- *the development of methods to promote the design and production of batteries that take into full account and facilitate the dismantling, reuse, recovery, and recycling of battery components and materials;*
- *strategies to increase consumer acceptance of, and participation in, the recycling of batteries;*
- *the extraction or recovery of critical minerals from batteries that are recycled;*

$60 million would be authorized for this program, and the federal share of projects can be no more than 50%.

DOE would be mandated to award $50 million in "grants, on a competitive basis, to States and units of local government to assist in the establishment or enhancement of State battery collection, recycling, and reprocessing programs."

DOE would administer a new "Battery Recycling and Second-Life Applications Program" that is, "a program of research, development, and demonstration of—

- *second-life applications for electric drive vehicle batteries that have been used to power electric drive vehicles; and*
- *technologies and processes for final recycling and disposal of the [aforementioned] devices*

The bill explains the purposes of this new program:

- *To improve the recycling rates and second-use adoption rates of electric drive vehicle batteries.*
- *To optimize the design and adaptability of electric drive vehicle batteries to make electric drive vehicle batteries more easily recyclable.*
- *To establish alternative supply chains for critical materials that are found in electric drive vehicle batteries.*
- *To reduce the cost of manufacturing, installation, purchase, operation, and maintenance of electric drive vehicle batteries.*

- *To improve the environmental impact of electric drive vehicle battery recycling processes.*

$200 million is appropriated for this program.
Finally, the Department of Energy must submit to Congress "a report that assesses using digital tools and platforms as climate solutions, including—

- *artificial intelligence and machine learning;*
- *blockchain technologies and distributed ledgers;*
- *crowdsourcing platforms;*
- *the Internet of Things;*
- *distributed computing for the grid; and*
- *software and systems."*

Bipartisan Infrastructure Package: DHS and CISA

The "Infrastructure Investment and Jobs Act" (H.R.3684), and the bill is now in the House. Yesterday, the House Rules Committee met to consider the legislative procedure for floor consideration and has scheduled another meeting for today on the same along with the FY 2022 budget resolution (S. Con. Res. 14) that will allow Democrats to proceed with the $3.5 trillion package to enact the White House's Build Back Better agenda and the "John R. Lewis Voting Rights Advancement Act of 2021" (H.R.4).

However, the path to House passage of H.R.3684 has been complicated by the insistence of 10 moderate House Democrats that Congress pass this bill before turning to the $3.5 trillion plan. Under normal circumstances, House Democrats can lose no more than three Democrats if no Republicans vote for a bill. House Speaker Nancy Pelosi (D-CA) has long been saying the House will not pass the infrastructure package before passing the larger bill through budget reconciliation. In part, Pelosi's position is informed by the opposition of liberals in her caucus of passing the infrastructure package first, allowing moderate Democrats to then possibly vote against the $3.5 trillion bill replete with policies that liberals tend to support more than moderates. House Democratic Leadership was trying to round up votes yesterday but apparently fell short as a vote on the three measures was pushed into today.

H.R. 3684 is teeming with technology funding and policy, the likes of which could alter United States (U.S.) policy in a number of realms for years to come. We looked at the broadband provisions (see here) and drinking water and electric grid provisions (see here) and today, we will examine the provisions and funding related to cybersecurity broadly speaking and any loose ends in the bill.

The Senate has opted to add funding for the newly established Office of the National Cyber Director (NCD) in the White House. There would be $21 million for the NCD, which may be in addition to what Congress may appropriate through the annual funding process. Alternatively, considering this is a bit more than one chamber has proposed for the NCD, Congress may not choose to appropriate any more funding to stand up and staff up this office.

In its FY 2022 budget request, the Biden Administration asked Congress for $15 million and 25 Full-Time Equivalents (FTE) to stand up the Office of the NCD. However, the CSC in making the recommendation that Congress create such a position called for at least 50 FTE in this office. Congress may appropriate funds and direct the creation of a larger office than the administration apparently wants. On 29 July, the House passed the "Financial Services and General Government Appropriations Act, 2022" (H.R.4502) that would make available $18.750 million for the NCD.

Additionally, last month, the Senate passed a bill, S.2382, "that would help ensure the newly created Office of the NCD will be able to quickly secure qualified personnel to support its important cybersecurity mission" according to the sponsors' press release. However, in late July, the House postponed floor proceedings to pass the bill under an expedited process until some later point in the future. It is possible if the House proposes its own package, this provision is added.

The Cybersecurity and Infrastructure Security Agency (CISA) would be given an additional $35 million "for risk management operations and stakeholder engagement and requirements."

The Department of Homeland Security's (DHS) Science and Technology Directorate (S&T) would be given $157.5 million "for critical infrastructure security and resilience research, development, test, and evaluation: Provided, That the funds made available under this heading in this Act may be used for

- *special event risk assessments rating planning tools;*
- *electromagnetic pulse and geo-magnetic disturbance resilience capabilities;*
- *positioning, navigation, and timing capabilities;*
- *public safety and violence prevention to evaluate soft target security, including countering improvised explosive device events and protection of U.S. critical infrastructure; and*
- *research supporting security testing capabilities relating to telecommunications equipment, industrial control systems, and open source software*

DHS would need to submit to Congress a detailed spending plan before these funds can be used.

H.R.3684 contains two discrete cybersecurity bills advanced in the last few months to counter the growing use of ransomware and penetration of federal networks.

The "State and Local Cybersecurity Improvement Act" (H.R.3138) would establish and fund with $1 billion a new grant program at DHS. The committee report for this House Homeland Security Committee bill explained:

H.R. 3138, the ''State and Local Cybersecurity Act,'' seeks to foster stronger partnerships between the Federal government and State and local governments to defend State and local networks against cyber attacks from sophisticated foreign adversaries or cyber criminals. It does so by authorizing a new Department of Homeland Security (DHS) grant program to address cybersecurity vulnerabilities on State and local government networks.

This bill would amend the section of the "Homeland Security Act of 2002" that established CISA (i.e. 6 U.S.C. 651, et. seq.) and establish the State and Local Cybersecurity Grant Program to help state and Tribal governments "to address cybersecurity risks and cybersecurity threats to information systems owned or operated by, or on behalf of, State, local, or Tribal governments." However, CISA will not administer the grant program; rather the Federal Emergency Management Agency (FEMA) will do so given its experience with other longstanding grant programs to state and Tribal governments.

State and Tribal governments that receive a grant "shall use the grant to—

- *implement the Cybersecurity Plan of the eligible entity;*
- *develop or revise the Cybersecurity Plan of the eligible entity;*
- *pay expenses directly relating to the administration of the grant, which shall not exceed 5 percent of the amount of the grant;*
- *assist with activities that address imminent cybersecurity threats, as confirmed by the Secretary, acting through the Director, to the information systems owned or operated by, or on behalf of, the eligible entity or a local government within the jurisdiction of the eligible entity; or*
- *fund any other appropriate activity determined by the Secretary, acting through the Director.*

Broadly speaking, recipient governments could fund Cybersecurity Plans or address imminent threats to their systems or those of local governments in their jurisdiction. These governments could also pull down 5% to administer the program and other appropriate activities CISA designates.

The Cybersecurity Plans would generally require governments to plan for cyber incidents and how they plan on recovering from them, including a continuous process of searching for and mitigating threats and vulnerabilities. These plans would also require the adoption and use of best practices. There is to be a risk-based approach with the greatest emphasis on the highest value systems and assets. In short, the sponsors of the legislation are hoping to use the power of Congress to condition the use of federal funds to drive better cybersecurity throughout the governments in the U.S.
Each eligible entity that wants to receive a grant must "establish a cybersecurity planning committee to—

- *assist with the development, implementation, and revision of the Cybersecurity Plan of the eligible entity;*
- *approve the Cybersecurity Plan of the eligible entity; and*
- *assist with the determination of effective funding priorities for a grant*

Moreover, DHS "may award grants under this section to a multi-entity group to support multi-entity efforts to address cybersecurity risks and cybersecurity threats to information systems within the jurisdictions of the eligible entities that comprise the multi-entity group." Multi-entity groups are those made up of two or more state or Tribal governments.

The bill appropriates $1 billion for this program in these allotments;

- for fiscal year 2022, $200,000,000;

- for fiscal year 2023, $400,000,000;
- for fiscal year 2024, $300,000,000; and
- for fiscal year 2025, $100,000,000.

The other bill folded into H.R. 3684, the "Cyber Response and Recovery Act of 2021" (S.1316), is legislation the sponsors claimed when it was introduced in April "would help improve the federal response to cyber breaches, such as recent and serious attacks by foreign adversaries including the Chinese and Russian governments that penetrated both federal networks and private companies' servers."

The first section of this bill explains its reason for being:

- *the purpose of this subtitle is to authorize the Secretary to declare that a significant incident has occurred and to establish the authorities that are provided under the declaration to respond to and recover from the significant incident; and*
- *the authorities established under this subtitle are intended to enable the Secretary to provide voluntary assistance to non-Federal entities impacted by a significant incident.*

The "Cyber Response and Recovery Act" adds a new term to the federal lexicon of cybersecurity: "significant incident," which is defined to be:

- *an incident or a group of related incidents that results, or is likely to result, in demonstrable harm to—*
  - *the national security interests, foreign relations, or economy of the United States; or*
  - *the public confidence, civil liberties, or public health and safety of the people of the United States; and*
- *does not include an incident or a portion of a group of related incidents that occurs on*
  - *a national security system (as defined in section 3552 of title 44, United States Code)[i.e. generally Department of Defense and Intelligence Community systems]; or*
  - *an information system described in paragraph (2) or (3) of section 3553(e) of title 44, United States Code*[1].

Congress has opted to define this term instead of delegating this responsibility to DHS and CISA as it sometimes does.

[1] (e) Department of Defense and Intelligence Community Systems.—
(2) The systems described in this paragraph are systems that are operated by the Department of Defense, a contractor of the Department of Defense, or another entity on behalf of the Department of Defense that processes any information the unauthorized access, use, disclosure, disruption, modification, or destruction of which would have a debilitating impact on the mission of the Department of Defense.
(3) The systems described in this paragraph are systems that are operated by an element of the intelligence community, a contractor of an element of the intelligence community, or another entity on behalf of an element of the intelligence community that processes any information the unauthorized access, use, disclosure, disruption, modification, or destruction of which would have a debilitating impact on the mission of an element of the intelligence community.

Under this bill, the definition for a mere "incident" is the one currently in the U.S. Code: "an occurrence that-

- *actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or*
- *constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.*

Clearly, significant incidents are those with much wider potential or actual repercussions than incidents.

DHS, in consultation with the NCD, "may make a declaration of a significant incident in accordance with this section for the purpose of enabling the activities described in this subtitle [more on this below] if the Secretary [of Homeland Security] determines that—

- *a specific significant incident—*
  - *has occurred; or*
  - *is likely to occur imminently; and*
- *otherwise available resources, other than the Fund* [more on this below]*, are likely insufficient to respond effectively to, or to mitigate effectively, the specific significant incident*

Moreover, the Secretary of Homeland Security may not delegate this responsibility to any other official. And so, this legislation contemplates that a Senate confirmed member of the Cabinet is the only official that may make the determination a significant incident has occurred. This was likely decided upon to keep decisions like this at the top of the U.S. government and made by an official who directly answers to both the President and Congress. Nonetheless, the NCD Chris Inglis, CISA Director Jen Easterly, and Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger, and others would play significant roles in the making of such a determination.

Significant incident declarations would last either 120 days or when the Secretary determines the declaration is no longer necessary, whichever comes first. The Secretary could extend the declaration if necessary. The Secretary must immediately alert the NCD and certain Congressional committees of a significant incident declaration, and this notification must estimate the expected duration, the reasons why the declaration was issued, the expected impact on federal and non-federal entities and on federal operations, the culprit (if known), the scope of those entities effected, justification for the resources to be used, and a description of the proposed coordination activities. Six months after a declaration or renewal, DHS must report to Congress on the actions taken, the funds expended, and the results.

And DHS must publish the declaration or a renewal of a declaration in the *Federal Register* within 72 hours of being made. However, any such declaration cannot include the name of any effected individual or company, which is a bit strange since any major incident will undoubtedly be widely reported upon.

After the Secretary has made this determination, DHS may must coordinate "asset response activities" which are defined as:

- *an activity to support an entity impacted by an incident with the response to, remediation of, or recovery from, the incident, including—*
    - *furnishing technical and advisory assistance to the entity to protect the assets of the entity, mitigate vulnerabilities, and reduce the related impacts;*
    - *assessing potential risks to the critical infrastructure sector or geographic region impacted by the incident, including potential cascading effects of the incident on other critical infrastructure sectors or geographic regions;*
    - *developing courses of action to mitigate the risks assessed…;*
    - *facilitating information sharing and operational coordination with entities performing threat response activities; and*
    - *providing guidance on how best to use Federal resources and capabilities in a timely, effective manner to speed recovery from the incident.*

In the aftermath of a significant incident declaration, DHS would coordinate the asset response activities of all federal agencies with a jurisdictional claim to the incident. DHS could also coordinate with public and private sector entities and state and local governments and law enforcement agencies as well.

Moreover, DHS need not wait for a significant incident declaration before acting. The agency may seek and obtain resources for asset response activities and technical assistance.

The bill establishes a Cyber Response and Recovery Fund (Fund) that shall, in part, finance the activities described in this section. DHS may also use the resources of CISA in responding to significant incidents. Money from the Fund could be provided to a range of effected entities on a reimbursable or non-reimbursable basis. CISA may also make "grants for, or cooperative agreements with, Federal, State, local, and Tribal public and private entities to respond to, and recover from, the specific significant incident associated with a declaration, such as—

- *hardware or software to replace, update, improve, harden, or enhance the functionality of existing hardware, software, or systems; and*
- *technical contract personnel support;*

Appropriations and reimbursements from other federal agencies would provide money for the Fund. $20 million is appropriated for this new program for each of the next five fiscal years, with the funding for two more fiscal years authorized. This program would end seven years after enactment unless Congress extends it.

There are finally transportation cybersecurity provisions. Within two years, the Federal Highway Administration (FHWA) "shall develop a tool to assist transportation authorities in identifying, detecting, protecting against, responding to, and recovering from cyber incidents." Transportation authorities include state highway departments and other transportation agencies, manufacturers of products related to transportation (a very broad term), and offices of the FHWA. The tool would need to use the National Institute of Standards and Technology's (NIST) cybersecurity framework, "establish a structured cybersecurity assessment and development program," be established in coordination with the Transportation Security Administration (TSA) and the Cybersecurity and Infrastructure

Security Administration (CISA), and be implemented only after consultation from stakeholders and a public comment period. The agency would also need "designate an office as a "cyber coordinator", which shall be responsible for monitoring, alerting, and advising transportation authorities of cyber incidents."

And for those skeptical of the effect of Government Accountability Office (GAO) reports and the like, the Department of Transportation (DOT) has three years to implement the GAO's recommendations from its report titled "Cybersecurity: Agencies Need to Fully Establish Risk Management Programs and Address Challenges." Specifically, the DOT must comply

- *by developing a cybersecurity risk management strategy for the systems and information of the Department;*
- *by updating policies to address an organization-wide risk assessment; and*
- *by updating the processes for coordination between cybersecurity risk management functions and enterprise risk management functions.*

The DOT would also need to implement recommendations made in a different GAO report "Cybersecurity Workforce: Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs" by

- *reviewing positions in the Department; and*
- *assigning appropriate work roles in accordance with the National Initiative for Cybersecurity Education Cybersecurity Workforce Framework.*

The GAO would then need to study and report on the DOT's "cybersecurity for the systems and information of the Department."